



#17
PATENT
8/17/04

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

EX PARTE

RECEIVED
APR 30 2004
GROUP 3600

Application for Patent

Applicant(s): Alain ROSSMANN, et al
Title: Method and Architecture for Providing Pervasive Security to
Digital Assets
Serial No.: 10/076,254
Confirmation No.: 8579
Filing Date: 02/12/2002
Examiner: Firmin Backer
Group Art Unit: 3621
Docket No: SS-004

APPEAL BRIEF

04/28/2004 MAHMED1 00000059 502107 10076254
01 FC:2402 165.00 DA

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the U.S. Postal Service with sufficient postage as first-class mail on April 23, 2004 in an envelope addressed to Mail Box: Appeal Brief-Patent, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signed:


Joe Zheng

April 23, 2004

TABLE OF CONTENTS

	<u>Page No.</u>
I. REAL PARTY IN INTEREST	1
II. RELATED APPEALS AND INTERFERENCES	1
III. STATUS OF CLAIMS	1
IV. STATUS OF AMENDMENTS	1
V. SUMMARY OF INVENTION	1
VI. ISSUES	3
VII. GROUPING OF CLAIMS	3
VIII. ARGUMENT	4
IX. CONCLUSION	11
X. APPENDIX	12



I. REAL PARTY IN INTEREST

PSS Systems, Inc. (formerly SecretSEAL, Inc.) located at 2471 East Bayshore Road, Suite 600, Palo Alto, CA 94303

II. RELATED APPEALS AND INTERFERENCES

None

III. STATUS OF THE CLAIMS

Claims 1-15, 17-62, 64-80 and 82-88 are now pending. On 02/23/2004, the Appellant appealed from the final rejections of Claim 1-15, 17-62, 64-80 and 82-88 that are rejected under 35 USC 103(a) as being unpatentable over Schenck et al (US Patent Publication No.: 2001/0021926) in view of Okamoto et al (US Application Publication No.: 2002/0129235), or in further view of Ozog et al (US Application Publication No.: 2003/0033528). These three cited references are referred to hereinafter as Schenck, Okamoto and Ozog, respectively.

IV. STATUS OF AMENDMENTS

Claims 1-88 were initially filed. In responding to a first Office Action, Claims 16, 63 and 81 were cancelled and Claims 1, 30, 31, 36, 41-43, 48, 67 and 78 were amended in a Response dated 5/20/2003. In responding to a second Office Action, Claims 1, 20, 31, 41, 47, 48, 67 and 78 have been amended in a Response dated 7/29/2003. There are no amendments in responding to a Final Office Action dated 11/4/2003. In the Advisory Action dated 02/02/2004, the Examiner simply indicates "argument not persuasive".

V. SUMMARY OF INVENTION

The invention relates to techniques for providing pervasive security to digital assets at all times. The examples of the digital assets include various types of documents, multimedia files, streaming data, dynamic or static data, executable code, images and texts. For simplicity, a digital asset is referred to as a file hereinafter. To ensure pervasive security of a file, the file is always secured in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to

RECEIVED

APR 30 2004

GROUP 3600

the encrypted data portion. Thus the secured file can be located anywhere, and can only be accessed by a user with proper privilege.

According to one embodiment, a server providing access control management manages a plurality of client machines and is never used to secure files. The server and the plurality of client machines may be in an enterprise environment. Thus after a file is created in a client machine, it can be secured in the format with access rules provided by a creator. The format includes security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion. When the secure file is being accessed by a user, the user has to be authenticated first. Once the user is authenticated, a user key associated with the user is activated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules.

According to another embodiment, the security information in a secured file includes security information controlling who, how, when or where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme. A pair of keys (e.g., a private key and a public key), both associated with a user, are maintained. The security information is encrypted with the public key in a client machine when the electronic data is to be written into a store (e.g., a hard disk); and the security information is decrypted with the private key in the client machine when the electronic data is to be accessed by an application (e.g., Microsoft Word). It is again noted that the client machine performs the encryption or decryption.

According to still another embodiment, when a request (from an application, such as a Microsoft Word, executed by a user) to access a file in a store, the file is intercepted on its way through an operating system (e.g., Windows XP) to the application, the security nature of the file is examined. When the security nature indicates that the file is secured, it is determined from the security information if the user has necessary access privilege in the operating system layer to access the encrypted data portion without consulting with another machine. A file key is retrieved from the security information to decrypt the encrypted data portion only

after the user is determined to have the necessary access privilege to access the encrypted data portion, and thereafter the application receives the electronic data in clear form.

According to still yet another embodiment, a storage device includes at least an active place designated for keeping files secured in a format including encrypted security information that further includes at least a set of access rules and a file key, wherein the access rules, expressed in a descriptive language, protects the file key and controls restrictive access to the secured electronic data. A client machine coupled to the storage device and executing a document securing module intercepts a secured file being requested. An access control server coupled to the client machine over a network receives a part of the secured file including the encrypted security information from the client machine, the encrypted security information is decrypted with a user key associated with a user attempting to access the file after both the user and the client machine are authenticated, wherein the set of access rules are measured against access privilege of the user in the access control server, if successful, the file key is returned to the client machine to facilitate a recovery of the electronic data in clear mode.

VI. ISSUES

The issues which Appellant believes to be most pertinent to the present appeal include:

- A. whether the Examiner failed to establish a *prima facie* case of obviousness. It is respectfully believed that the Final Action as well as the Advisory Action failed to consider each recited elements in claim 1, 20, 31, 41, 47, 48, 67 and 78 and did not show how each element is taught in the prior art. The Actions also failed to consider the recited limitations in the various dependent claims that were rejected based on non-related parts in the cited references.

VII. GROUPING OF CLAIMS

With respect to issue A, the rejected claims do not stand or fall together. Currently Claims 1, 20, 31, 41, 47, 48, 67 and 78 are independent claims.

Accordingly, Claims 1 and 48 together with corresponding dependent claims will be argued as a first group, Claims 20 and 67 together with corresponding dependent claims will be argued as a second group, Claims 31, 41 and 78 together with corresponding dependent claims will be argued as a third group, and the remaining Claim 47 will be argued as a fourth group.

VIII. ARGUMENT

Patentability of Claims 1 and 48

Claim 1 is rejected under 35 USC 103(a) as being unpatentable by Schenck in view of Okamoto. The Appellant respectfully traverses the rejection.

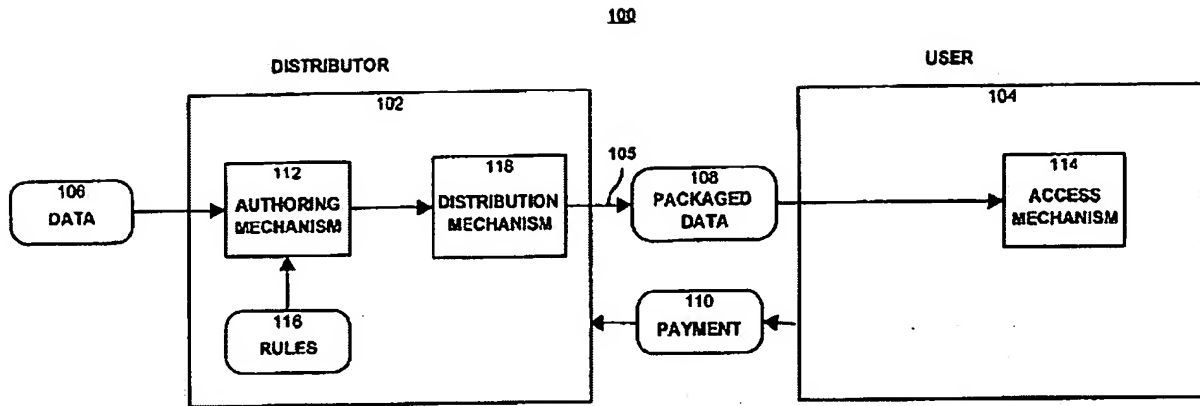
It is axiomatic that an invention in a patent application is defined by, and must be examined with respect to, the specific language in the claims. Specific and distinct feature(s) in Claim 1 is set forth below:

establishing a secured link between a server providing the access control management and a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is not from the server but secured in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion;
authenticating the user according to the identifier; and
activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules.

(emphasis added)

As described in the above section "SUMMARY OF INVENTION" and the pending application, the server recited in Claim 1 provides access control management and manages a plurality of client machines and is never used to secure files. Further, the file is not from the server.

In contrast, as shown in FIG. 1 of Schenck which is duplicated below for the convenience of the Examiners involved:



The corresponding description of FIG. 1 in Schenck is provided (see Col. 2, paragraphs 0086 and 0087), *data 106 is encrypted in the distributor 102 and sent as packaged data 108 to a user 104 after a payment 110*. In other words, Schenck provides an on-demand data method. As clearly shown in the figure, a server or the distributor 102 is configured to encrypt demanded data and transmit the demanded data in encryption to a demander (i.e., a user), namely, the data 106 must be encrypted in and from the distributor 102. The authorizing mechanism 112 and rules 116 in distributor 102 are clearly shown to achieve the encryption of the data 106.

Evidently, comparing "wherein the electronic data is not from the server but secured in a format including security information and an encrypted data portion" recited in Claim 1 with Schenck, the Appellant respectfully submits such features are neither taught nor suggested in Schenck. In fact, Schenck teaches away from the recited feature in Claim 1. If a server was used to secure a file like in Schenck, the present invention would contradict one aspect of "a server providing access control management manages a plurality of client machines and is never used to secure files".

Besides the above distinctions, it is believed that the Examiner also failed to consider limitations "activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules" (*emphasis added*) Evidently, none of the cited paragraphs 0049, 0053, 0060, 0086 and 0087 by the Examiner and other description in Schenck teach or suggest such limitations.

Based on the above-noted differences, Claim 1 and corresponding dependent claims 2-15 and 17-19 shall be allowable over Schenck and Okamoto, viewed alone or in combination. Since Claim 48 recites similar features of Claim 1, the Appellant wishes to apply the above arguments to support Claim 48. Therefore, it is believed that Claims 48 - 62 and 64 - 66 should be allowable as well.

Patentability of Claims 20 and 67

Claim 20 is rejected under 35 USC 103(a) as being unpatentable by Schenck in view of Okamoto. The Appellant respectfully traverses the rejection.

It is axiomatic that an invention in a patent application is defined by, and must be examined with respect to, the specific language in the claims. Specific and distinct feature(s) in Claim 20 is set forth below:

authenticating a user attempting to access the electronic data;
maintaining a private key and a public key, both associated with the user,
wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when or where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme;
encrypting the security information with the public key in the client machine when the electronic data is to be written into a store; and
decrypting the security information with the private key in the client machine when the electronic data is to be accessed by an application.

(emphasis added)

Claim 20 clearly recites that there are two keys associated with a user attempting to access electronic data (e.g., a secured file). Further it shows "encrypting the security information with the public key in the client machine when the electronic data is to be written into a store" and "decrypting the security information with the private key in the client machine when the electronic data is to be accessed by an application". Evidently, the user must be present (identified) and the pair of keys associated with the user must be available in a client machine to be used for encryption or decryption.

Evidently, the above figure duplicated from Schenck on P. 5 contradicts "encrypting the security information with the public key in the client machine when

the electronic data is to be written into a store” because, per Schenck, *data 106 is encrypted in the distributor 102 and sent as packaged data 108 to a user 104 after a payment 110*. Further, the Examiner cites Schenck to reject Claim 20 by referring to Figures 1 and 2, and paragraphs 0049, 0053, 0060, 0086 and 0087 in Schenck. A careful review of these cited paragraphs in conjunction with Figures 1 and 2 and other paragraphs of Schenck shows that Schenck is silent on a pair of keys associated with the user and available for both encryption and decryption in a client machine. There is no any teaching in Schenck, particularly in these cited paragraphs 0049, 0053, 0060, 0086 and 0087 in Schenck, that a key associated with the user is used in encryption of the data 106 in a client machine because Schenck dictates in FIG.1 that the distributor 102 does the encryption.

Based on the above-noted differences, Claim 20 and corresponding dependent claims 21-30 shall be allowable over Schenck and Okamoto, viewed alone or in combination. Since Claim 67 recites similar features of Claim 20, the Appellant wishes to apply the above arguments to support Claim 67, and therefore it is believed that Claims 67 - 77 should be allowable as well.

Patentability of Claim 31, 41 and 78

Claim 31 is rejected under 35 USC 103(a) as being unpatentable by Schenck in view of Okamoto. The Appellant respectfully traverses the rejection.

It is axiomatic that an invention in a patent application is defined by, and must be examined with respect to, the specific language in the claims. Specific and distinct feature(s) in Claim 31 is set forth below:

- receiving a request to access the electronic data in a store;
- determining security nature of the electronic data by intercepting the electronic data moving from the store through an operating system layer to an application for the data;
- when the security nature indicates that the electronic data is secured, the electronic data including a header and an encrypted data portion, the header including security information controlling restrictive access to the encrypted data portion and the encrypted data portion including an encrypted version of the electronic data according to a predetermined cipher scheme,

determining from the security information if the user has necessary access privilege in the operating system layer to access the encrypted data portion without consulting with another machine; and obtaining a file key and decrypting the encrypted data portion with the file key only after the user is determined to have the necessary access privilege to access the encrypted data portion, and thereafter the application receives the electronic data in clear form.

(emphasis added)

To better understand the features recited in Claim 31, FIG. 3 of the current application is duplicated herein below, wherein it supports that a file (e.g., the

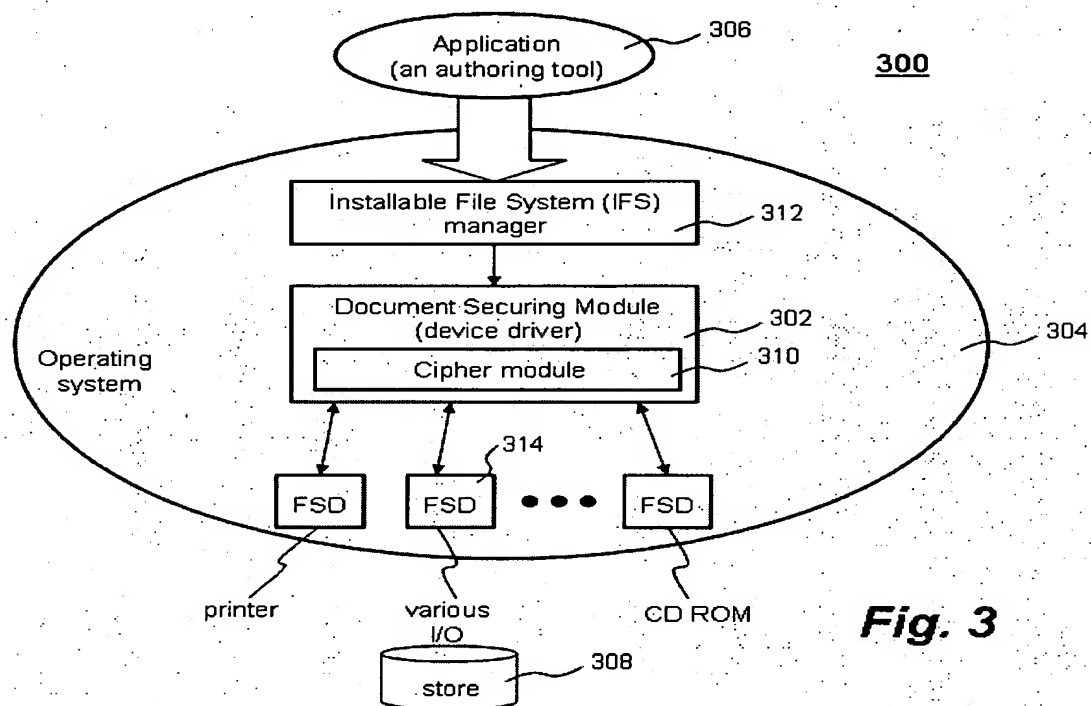


Fig. 3

electronic data) stored in a store 308, when passing through the operating system 304 is intercepted (by the document securing module 302) to determine the security nature of the file. If it is in secured format, the file will be processed accordingly (by the document securing module 302). It should be noted that, in conjunction with the description of FIG. 1D, FIG. 3 is a functional layer diagram of a client machine (e.g., a desktop computer) running on the operating system 304, on top of which is an application 306 (e.g., a Microsoft Word), and having a store 308 e.g., a hard disk). A typical example is to execute Microsoft Word to access a file in the store. When the file is retrieved from the store through the operating system, the file gets intercepted. The above is all provided in the description of the current application.

The Examiner has admitted in lines 2-4 of page 4 in the Final Office Action that Schenck fails to teach the inventive concept of intercepting (an) electronic data moving from the store through an operating system layer to an application for the data, and thus cites paragraphs 0016, 0017 and 0018 of Okamoto to reject such features recited in Claim 31. Interestingly, the Appellant could not find any relevance of these paragraphs to the feature recited in Claim 31. In fact, Okamoto never teaches or suggests an operating system, or uses the word phrase “operating system” in the system being disclosed. Okamoto provides a system in which a plurality of devices having different structures can receive various services without taking into consideration the difference in the structure, by conducting administration of rights of digital data at a server. In particular, Okamoto discloses various considerations between a server and a receiving device, which is not remotely related to what is recited in Claim 31 of the current application. Accordingly, the Appellant respectfully submits that Claim 31 is neither taught nor suggested in Schenck and Okamoto, viewed alone or in combination.

Based on the above-noted differences, Claim 31 and corresponding dependent claims 32 - 40 shall be allowable over Schenck and Okamoto. Since Claim 78 recites similar features of Claim 31, the Appellant wish to apply the above arguments to support Claim 78, and therefore it is believed that Claims 78 - 80 and 82 - 88 should be allowable as well.

Claim 41 is a system claim and rejected without specific reasons. Claim 41 particularly recites “a document securing module that operates in a path through which the electronic data is caused to pass when selected, the document securing module determining security nature of the electronic data” which is similarly supported in FIG. 3 duplicated above, namely the electronic data is intercepted by the document securing module. As the Examiner has admitted in lines 2-4 of page 4 in the Final Office Action that Schenck fails to teach the inventive concept of intercepting (an) electronic data moving from the store through an operating system layer to an application for the data, with the above arguments that Okamoto fails to disclose the same, it is believed that Claim 41 and corresponding dependent claims 42 – 46 shall be allowable over Schenck and Okamoto, viewed alone or in combination.

Patentability of Claim 47

Claim 47 is an independent claim without any dependent claims and rejected under the same rationale without any specific reasons. The Appellant respectfully traverses such rejection.

Claim 47 recites:

a storage device including at least an active place designated for keeping the electronic data secured, the secured electronic data including encrypted security information that further includes at least a set of access rules and a file key, wherein the access rules, expressed in a descriptive language, protects the file key and controls restrictive access to the secured electronic data;

a client machine coupled to the storage device and executing a document securing module operative to intercept the electronic data when the electronic data is caused to transport from the active place;

an access control server coupled to the client machine over a network and receiving a part of the electronic data including the encrypted security information from the client machine, the encrypted security information being decrypted with a user key associated with a user attempting to access the electronic data after both the user and the client machine are authenticated;

wherein the set of access rules are measured against access privilege of the user in the access control server, if successful, the file key is returned to the client machine to facilitate a recovery of the electronic data in clear mode.

Evidently, Claim 47, being a system claim, is related to a different embodiment of the present invention. In particular, Claim 47 recites only a portion of a secured file (i.e. secured electronic data) being transported to an access control server that is configured to decrypt that portion with a user key associated with a user attempting to access the secured file. Assumed that the decryption is successful, a file key from that portion of the secured file is returned to a client machine being used by the user to recover the secured file in clear mode. The

Appellant respectfully submit these combined features are neither taught nor suggested in Schenck and Okamoto, viewed alone or in combination. Therefore it is believed that Claim 47 should be allowable over the cited references.

XI. CONCLUSION

The Examiner is respectfully believed to have failed to set forth a *prima facie* case of obviousness. It is the burden of the Examiner to establish why one having ordinary skill in the art would have been led to the claimed invention by the express teachings or suggestions found in the cited references, or by implications contained in such teachings or suggestions. In re Sernaker, 702 F.2d 989, 995, 217 USPQ 1, 6 (Fed. Cir. 1983). "Additionally, when determining obviousness, the claimed invention should be considered as a whole; there is no legally recognizable 'heart' of the invention." The Examiner makes no specific statements on the limitations recited in the independent claims, and the cited paragraphs as well as the description of the cited references either fail to show or silent on the limitations. It respectfully believed that the Examiner provides a broad unsupported general conclusion of obviousness.

In view of the foregoing, it is respectfully submitted that the combined features in Claims 1-15, 17-62, 64-80 and 82-88 are neither taught nor suggested in any of the cited references, viewed alone or in combination. Accordingly, the pending rejections of all of the claims under 35 USC 103(a) should be reversed.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to " Mail Stop: Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450", on April 23, 2004.

Name: Joe Zheng

Signature: 

Respectfully Submitted,



Joe Zheng

Reg. No.: 39,450

Tel: (408)777-8873

X. APPENDIX

CLAIMS ON APPEAL

1. *(Previously amended)* A method for providing access control management to electronic data, the method comprising:
 - establishing a secured link between a server providing the access control management and a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is not from the server but secured in a format including security information and an encrypted data portion, the security information including a file key and access rules and controlling restrictive access to the encrypted data portion;
 - authenticating the user according to the identifier; and
 - activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules.
2. *(Original)* The method as recited in Claim 1 further comprising maintaining an access control management, wherein the access control management comprises:
 - a rule manager including at least one set of rules for the electronic data; and
 - an administration interface from which the rules for a designated place for the electronic data are created, managed, or updated.
3. *(Previously amended)* The method as recited in Claim 2, wherein the designated place is a folder and all files in the folder are subject to the rules.
4. *(Previously amended)* The method as recited in Claim 2, wherein the designated place is a repository and all files in the repository are subject to the rules.

5. *(Previously amended)* The method as recited in Claim 2, wherein the rule manager provides a graphic user interface from which the rules can be created, managed or updated.
6. *(Previously amended)* The method as recited in Claim 5, wherein parameters determining the rules from the graphic user interface are subsequently expressed in a markup language.
7. *(Previously amended)* The method as recited in Claim 6, wherein the parameters expressed in the markup language are uploaded to the client machine after the user is authenticated.
8. *(Previously amended)* The method as recited in Claim 7, wherein the markup language is Extensible Access Control Markup Language.
9. *(Original)* The method as recited in Claim 7, wherein the markup language is selected from a group consisting of HTML, XML and SGML.
10. *(Original)* The method as recited in Claim 2, wherein the access control management further comprises a user manager coupled to a database including a list of authorized users and respective access privileges associated with each of the authorized users.
11. *(Original)* The method as recited in Claim 10, wherein the authenticating of the user comprises:
 - looking up in the database for the user; and
 - getting, from the database, access location information as to where the user is authorized to access the electronic data if information about the user is located in the database.
12. *(Original)* The method as recited in Claim 11, wherein the identifier further identifies the client machine; and wherein the authenticating of the user

comprises determining, from the access location information, whether the client machine is permitted by the user to access the electronic data.

13. (*Previously amended*) The method as recited in Claim 11, wherein the access location information pertains to locations or specific client machines from which the user is authorized to access the electronic data.

14. (*Original*) The method as recited in Claim 1, wherein the user key is in the client machine; and wherein the activating of the user key comprises:
 sending an authentication message to the client machine; and
 activating the user key with the authentication message.

15. (*Previously amended*) The method as recited in Claim 14, wherein the electronic data, when secured, includes a header that further includes the security information being encrypted and a signature signifying that the electronic data is secured.

16. (*Cancelled*)

17. (*Original*) The method as recited in Claim 1 further comprising associating the activated user key with the user locally.

18. (*Previously amended*) The method as recited in Claim 17, wherein the electronic data, when secured, includes a header that includes the security information being encrypted and a signature signifying that the electronic data is secured; the encrypted security information including the access rules and a file key, and wherein the method further comprises:
 receiving the header from the client machine;
 decrypting the security information in the header to retrieve the access rules therein; and
 retrieving the file key when the access rules are measured successfully against access privilege of the user.

19. *(Original)* The method as recited in Claim 18 further comprising sending the file key to the client machine in which the encrypted data portion can be decrypted with the file key by a cipher module executing in the client machine.
20. *(Previously amended)* A method for providing access control management to electronic data in a client machine, the method comprising:
 authenticating a user attempting to access the electronic data;
 maintaining a private key and a public key, both associated with the user,
 wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when or where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme;
 encrypting the security information with the public key in the client machine when the electronic data is to be written into a store; and
 decrypting the security information with the private key in the client machine when the electronic data is to be accessed by an application.
21. *(Previously amended)* The method as recited in Claim 20, wherein the authentication of the user comprises:
 establishing a link with the client machine from which the user is attempting to access the electronic data;
 demanding credential information from the user; and
 receiving the credential information from the client machine over the link.
22. *(Original)* The method as recited in Claim 21, wherein the credential information includes a pair of username and password provided by the user.
23. *(Original)* The method as recited in Claim 21, wherein the credential information includes biometric information captured from the user by an apparatus coupled to the client machine.

24. *(Previously amended)* The method as recited in Claim 21, wherein the encrypting of the security information with the public key comprises:
- receiving access rules and a file key, wherein the file key has been used to produce the encrypted data portion in the client machine;
 - including the access rules and the file key into the security information; and
 - encrypting the security information with the public key.
25. *(Original)* The method as recited in Claim 24 further comprising:
- generating the header with the security information encrypted therein; and
 - uploading the header to the client machine where the header is integrated with the encrypted data portion.
26. *(Original)* The method as recited in Claim 24, wherein the access rules are expressed in a markup language.
27. *(Original)* The method as recited in Claim 26, wherein the markup language is one of Extensible Access Control Markup Language, HTML, XML and SGML.
28. *(Original)* The method as recited in Claim 21, wherein the decrypting of the security information with the private key comprises:
- receiving the header from the client machine over the link;
 - parsing the security information from the header; and
 - decrypting the security information with the private key.
29. *(Original)* The method as recited in Claim 28 further comprising:
- obtaining access rules from the security information;
 - determining whether the access rules accommodate access privilege of the user;
 - when the determining succeeds,
 - retrieving a file key from the security information; and
 - sending the file key to the client machine over the link.
 - when the determining fails,
 - sending an error message to the client machine over the link.

30. *(Previously amended)* The method as recited in Claim 29, wherein the error message indicates that the user does not have the access privilege to access the electronic data.

31. *(Previously amended)* A method for providing access control management to electronic data, the method comprising:

- receiving a request to access the electronic data in a store;
- determining security nature of the electronic data by intercepting the electronic data moving from the store through an operating system layer to an application for the data;
- when the security nature indicates that the electronic data is secured, the electronic data including a header and an encrypted data portion, the header including security information controlling restrictive access to the encrypted data portion and the encrypted data portion including an encrypted version of the electronic data according to a predetermined cipher scheme,
- determining from the security information if the user has necessary access privilege in the operating system layer to access the encrypted data portion without consulting with another machine; and
- obtaining a file key and decrypting the encrypted data portion with the file key only after the user is determined to have the necessary access privilege to access the encrypted data portion, and
- thereafter the application receives the electronic data in clear form.

32. *(Original)* The method as recited in Claim 31 further comprising retrieving a user key associated with a user making the request.

33. *(Original)* The method as recited in Claim 32 wherein said determining from the security information if the user has necessary access privilege comprises:

- decrypting the security information with the user key;
- retrieving access rules from the security information; and
- measuring the access rules against the access privilege of the user.

34. *(Original)* The method as recited in Claim 33 further comprising:
retrieving the file key from the security information if the measuring of the
access rules against the access privilege succeeds.
35. *(Original)* The method as recited in Claim 33 further comprising:
causing the client machine to display an error message to the user if the
measuring of the access rules against the access privilege fails.
36. *(Previously amended)* The method as recited in Claim 32, wherein the retrieving
of the user key comprises:
establishing a link with a server executing an access control management;
sending to the server an authentication request including an identifier
identifying the user for the access control management to authenticate the
user;
forwarding the header to the server; and
receiving the file key retrieved from the header.
37. *(Original)* The method as recited in Claim 36 further comprising:
activating a cipher module; and
decrypting the encrypted data portion by the cipher module with the received
file key.
38. *(Original)* The method as recited in Claim 37 further comprising loading the
decrypted data portion into the application.
39. *(Original)* The method as recited in Claim 32, wherein the retrieving of the user
key comprises:
establishing a link with a server executing an access control management;
sending to the server an authentication request including an identifier
identifying the user for the access control management to authenticate the
user;
receiving an authentication message after the user is authenticated; and

activating the user key locally in the client machine.

40. *(Original)* The method as recited in Claim 39, wherein the user key is in an illegible format before the activating of the user key locally in the client machine.

41. *(Previously amended)* A system for providing access control management to electronic data, the system comprising:

- a client machine executing a document securing module that operates in a path through which the electronic data is caused to pass when selected, the document securing module determining security nature of the electronic data,

- an access control server coupled to the client machine over a network, the access control server including an account manager managing all users who access the electronic data; and

- wherein the client machine and a user thereof are caused by the document securing module to be authenticated with the access control server when the security nature indicates that the electronic data is secured; and
- wherein access rules in the secured electronic data are retrieved with a user key associated with the user to test against access privilege of the user to determine if the user can access the secured electronic data.

42. *(Previously amended)* The system as recited in Claim 41, wherein the access privilege of the user is also tested against other rules imposed by the system.

43. *(Previously amended)* The system as recited in Claim 41, wherein the document securing module activates a cipher module to decrypt an encrypted data portion in the secured electronic data with a file key obtained therefrom after the document securing module determines that the access privilege of the user is permitted by the access rules.

44. *(Previously amended)* The system as recited in Claim 43, wherein the user key stays in the access control server that receives part of the secured electronic

data; and wherein the access rules and the file key are obtained from the part of the secured electronic data

45. *(Previously amended)* The system as recited in Claim 44, wherein the access control server forwards the file key to the client machine in a secured form over the network.

46. *(Previously amended)* The system as recited in Claim 43, wherein the user key stays in the client machine and is activated when both the client machine and the user are authenticated by the access control server.

47. *(Previously amended)* A system for providing access control management to electronic data, the system comprising:

- a storage device including at least an active place designated for keeping the electronic data secured, the secured electronic data including encrypted security information that further includes at least a set of access rules and a file key, wherein the access rules, expressed in a descriptive language, protects the file key and controls restrictive access to the secured electronic data;

- a client machine coupled to the storage device and executing a document securing module operative to intercept the electronic data when the electronic data is caused to transport from the active place;

- an access control server coupled to the client machine over a network and receiving a part of the electronic data including the encrypted security information from the client machine, the encrypted security information being decrypted with a user key associated with a user attempting to access the electronic data after both the user and the client machine are authenticated;

wherein the set of access rules are measured against access privilege of the user in the access control server, if successful, the file key is returned to the client machine to facilitate a recovery of the electronic data in clear mode.

48. *(Previously amended)* A software product to be executable in a computing device for providing access control management to electronic data, the software product comprising:

program code for establishing a secured link between a server supporting the access control management and a client machine when an authentication request is received therefrom, the authentication request including an identifier identifying a user from the client machine to access the electronic data not received from the server but in a secured format including a file key and security information and an encrypted data, the security information including access rules and controlling restrictive access to the encrypted data portion;

program code for authenticating the user according to the identifier; and

program code for activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules.

49. *(Previously amended)* The software product as recited in Claim 48 further comprising program code for maintaining an access control management, wherein the access control management comprises:

a rule manager including at least one set of rules for the electronic data; and
an administration interface from which the rules for a designated place for the electronic data are created, managed or updated.

50. *(Previously amended)* The software product as recited in Claim 49, wherein the designated place is a folder and all files in the folder are subject to the rules.

51. *(Previously amended)* The software product as recited in Claim 47, wherein the designated place is a repository and all files in the repository are subject to the rules.

52. *(Previously amended)* The software product as recited in Claim 47, wherein the rule manager provides a graphic user interface from which the rules can be created, managed or updated.
53. *(Previously amended)* The software product as recited in Claim 52, wherein parameters determining the rules from the graphic user interface are subsequently expressed in a markup language.
54. *(Previously amended)* The software product as recited in Claim 53, wherein the parameters expressed in the markup language are uploaded to the client machine after the authenticating of the user succeeds.
55. *(Previously amended)* The software product as recited in Claim 54, wherein the markup language is Extensible Access Control Markup Language.
56. *(Original)* The software product as recited in Claim 54, wherein the markup language is selected from a group consisting of HTML, XML and SGML.
57. *(Original)* The software product as recited in Claim 49, wherein the access control management further comprises a user manager coupled to a database including a list of authorized users and respective access privileges associated with each of the authorized users.
58. *(Original)* The software product as recited in Claim 57, wherein the program code for authenticating the user comprises:
 program code for looking up in the database for the user; and
 program code for getting, from the database, access location information as to where the user is authorized to access the electronic data if the user is located in the database.
59. *(Original)* The software product as recited in Claim 58, wherein the identifier further identifies the client machine; and wherein the program code for authenticating the user comprises program code for determining, from the access

location information, whether the client machine is permitted by the user to access the electronic data.

60. *(Previously amended)* The software product as recited in Claim 58, wherein the access location information pertains to locations or specific client machines from which the user is authorized to access the electronic data.

61. *(Original)* The software product as recited in Claim 48, wherein the user key is in the client machine; and wherein the program code for activating the user key comprises:

program code for sending an authentication message to the client machine;

and

program code for activating the user key with the authentication message.

62. *(Original)* The software product as recited in Claim 61, wherein the electronic data, when secured, includes a header and an encrypted data portion; and wherein the header includes security information that can be accessed with the activated user key.

63. *(Cancelled)*

64. *(Original)* The software product as recited in Claim 48 further comprising program code for associating the activated user key with the user locally.

65. *(Original)* The software product as recited in Claim 64, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header includes security information and a file key; and wherein the software product further comprises:

program code for receiving the header from the client machine;

program code for decrypting the header to retrieve access rules in the security information; and

program code for retrieving the file key when the access rules are measured successfully against access privilege of the user.

66. (*Original*) The software product as recited in Claim 65 further comprising sending the file key to the client machine in which the encrypted data portion can be decrypted with the file key by a cipher module executing in the client machine.

67. (*Previously amended*) A software product to be executable in a computing device for providing access control management to electronic data in a client machine, the software product comprising:

- program code for authenticating a user attempting to access the electronic data;

- program code for maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling restrictive access to the encrypted data portion and protecting the private key by access rules therein;

- program code for encrypting the security information with the public key in the client machine when the electronic data is to be written into a store; and

- program code for decrypting the security information with the private key in the client machine when the electronic data is to be accessed by an application.

68. (*Previously amended*) The software product as recited in Claim 67, wherein the program code for authenticating the user comprises:

- program code for establishing a link with the client machine from which the user is attempting to access the electronic data;

- program code for demanding credential information from the user; and

- program code for receiving the credential information from the client machine over the secured link.

69. (*Original*) The software product as recited in Claim 68, wherein the credential information includes a pair of username and password provided by the user.

70. *(Original)* The software product as recited in Claim 68, wherein the credential information includes biometric information captured from the user by an apparatus coupled to the client machine.
71. *(Previously amended)* The software product as recited in Claim 68, wherein the program code for encrypting the security information with the public key comprises:
- program code for receiving the access rules and a file key from the client machine over the link, wherein the file key has been used to produce the encrypted data portion in the client machine;
 - program code for including the access rules and a file key into the security information; and
 - program code for encrypting the security information with the public key.
72. *(Original)* The software product as recited in Claim 71 further comprising:
- program code for generating the header with the security information encrypted therein; and
 - program code for uploading the header to the client machine where the header is integrated with the encrypted data portion.
73. *(Original)* The software product as recited in Claim 74, wherein the access rules are expressed in a markup language.
74. *(Original)* The software product as recited in Claim 73, wherein the markup language is one of Extensible Access Control Markup Language, HTML, XML and SGML.
75. *(Original)* The software product as recited in Claim 68, wherein the program code for decrypting the security information with the private key comprises:
- program code for receiving the header from the client machine over the link;
 - program code for parsing the security information from the header; and
 - program code for decrypting the security information with the private key.

76. *(Original)* The software product as recited in Claim 75 further comprising:
program code for obtaining access rules from the security information;
program code for determining whether the access rules accommodate access
privilege of the user;
when the determining program code is executed successfully,
program code for retrieving a file from the security information; and
program code for sending the file key to the client machine over the link.
when the determining program code is executed unsuccessfully,
program code for sending an error message to the client machine over the
link.

77. *(Original)* The software product as recited in Claim 76 wherein the error message
indicate that the user does not have the access privilege to access the electronic
data.

78. *(Previously amended)* A software product to be executable in a computing device
for providing access control management to electronic data, the software product
comprising:

program code for receiving a request to access the electronic data in a store;
program code for determining security nature of the electronic data by
intercepting the electronic data moving from the store through an operating
system layer to an application for the data;

when the security nature indicates that the electronic data is secured, wherein
the electronic data including a header and an encrypted data portion, the
header including security information and the encrypted data portion
including an encrypted version of the electronic data according to a
predetermined encryption scheme,

program code for determining from the security information if the user
has necessary access privilege in the operating system layer to
access the encrypted data portion; and

program code for a file key from the security information and decrypting
the encrypted data portion only after the access privilege of the user

is permitted in view of the security information, and thereafter the application receives the electronic data in clear form.

79. *(Original)* The software product as recited in Claim 78 further comprising program code for retrieving a user key associated with a user making the request.

80. *(Original)* The software product as recited in Claim 79 wherein the program code for determining from the security information, if the user has necessary access privilege, comprises:

- program code for decrypting the security information with the user key;
- program code for retrieving access rules from the security information; and
- program code for measuring the access rules against the access privilege of the user.

81. *(Cancelled)*

82. *(Original)* The software product as recited in Claim 80 further comprising:

- program code for causing the client machine to display an error message to the user if the measuring of the access rules against the access privilege fails.

83. *(Original)* The software product as recited in Claim 80, wherein the program code for retrieving the user key comprises:

- program code for establishing a link with a server executing an access control management;
- program code for sending to the server an authentication request including an identifier identifying the user for the access control management to authenticate the user;
- program code for forwarding the header to the server; and
- program code for receiving a file key retrieved from the header.

84. *(Original)* The software product as recited in Claim 83 further comprising:
program code for activating a cipher module; and

program code for decrypting the encrypted data portion by the cipher module with the received file key.

85. *(Original)* The software product as recited in Claim 84 further comprising program code for loading the decrypted data portion into the application.

86. *(Original)* The software product as recited in Claim 79, wherein the program code for retrieving the user key comprises:

program code for establishing a link with a server executing an access control management;

program code for sending to the server an authentication request including an identifier identifying the user for the access control management to authenticate the user;

program code for receiving an authentication message after the user is authenticated; and

program code for activating the user key locally in the client machine.

87. *(Original)* The software product as recited in Claim 86, wherein the user key is in an illegible format before the activating of the user key locally in the client machine.

88. *(Original)* The software product as recited in Claim 86, wherein the computing device is a media player having a network capacity, the media player generating audio and/or video from the electronic data when the software product is executed in the media player.



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Alain ROSSMANN, et al
Title: Method and Architecture for Providing Pervasive Security to
Digital Assets
Serial No.: 10/076,254
Confirmation No.: 8579
Filing Date: 02/12/2002
Examiner: Firmin Backer
Group Art Unit: 3621
Docket No: SS-004

RECEIVED
APR 30 2004
GROUP 3600

April 23, 2004

Mail Stop: Notice of Appeal
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Request to Correct Date Entries in PAIR Record
(Filed concurrently with APPEAL BRIEF)

Dear Sir:

A call was received from the Examiner to indicate that the case is to be abandoned because of failure of any response to the Final Office Action/Adversary Action. After reviewing the PAIR record, the undersigned noticed there were a number of incorrect entries in the PAIR record that may have caused a wrong status of the current application.

The undersigned respectfully requests the incorrect entries be reversed in accordance with the supporting materials enclosed hereinwith:

1. The date of Response to the Final Office Action dated 10/14/2003 should be November 4, 2003. The current PAIR record shows the

Response was filed 01/10/2004. Exhibit A includes 7 pages to show the Response was faxed on 11/4/2003 and a fax Journal printout shows the 6-page Response was successfully faxed to USPTO fax No.: (703)305-7687.

2. The date of Notice of Appeal after the Advisory Action dated 02/02/2004 should be 02/23/2004. The current PAIR record does not show such entry. Exhibit B includes 4 pages to show a Facsimile Transmittal Sheet, a Notice of Appeal, and an Auto-Reply Facsimile Transmission from USPTO.

Remarks

It is assumed that the Commissioner will authorize the PAIR record to be corrected. As a result of these corrections, the Period for reply to the Final Office Action expires on the mailing date of the Advisory Action. The one-month extension on the Notice of Appeal is correctly requested.

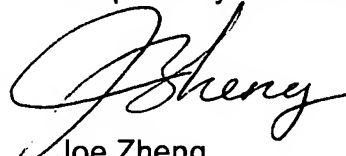
The undersigned can be reached at (408)777-8873 if there is any question.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to "Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450", on April. 23, 2004.

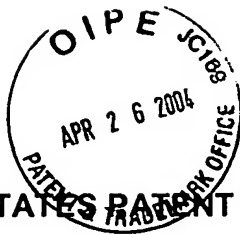
Name: Joe Zheng

Signature: 

Respectfully submitted;


Joe Zheng
Reg.: No. 39,450

63



AF
1362V
AK

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): Alain ROSSMANN, et al
Title: Method and Architecture for Providing Pervasive Security to Digital Assets
Serial No.: 10/076,254
Confirmation No.: 8579
Filing Date: 02/12/2002
Examiner: Firmin Backer
Group Art Unit: 3621
Docket No: SS-004

April 23, 2004

Mail Stop: Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RECEIVED
APR 30 2004
GROUP 3600

APPEAL BRIEF TRANSMITTAL
(37 CFR 1.192)

Dear Sir:

This Appeal Brief is in furtherance of the Notice of Appeal filed in this case on 02/23/2004. This Appeal Brief is transmitted in triplicate.

The item(s) checked below are appropriate:

- ☒ This application is on behalf of: ☒ Small Entity ☐ Large Entity
- ☒ The fee for filing the Appeal Brief: \$165.00 (Small Entity).
- ☐ Extension of time fee amount \$ (Small Entity).
- a. ☐ Enclosed.

Del.
165.00
42604

b. [] Charge to Deposit Account No.: 502107 (Order No.: SS-004)

The Applicant believes that no (additional) extension of time is required, however, if it is determined that such an extension is required, the Applicant hereby petitions that such an extension be granted and The Commission is authorized to charge the required fees to the Deposit Account No.: 502107.

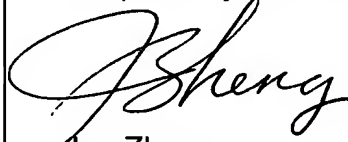
The Commissioner is authorized to charge Deposit Account No.: 502107 any fees that may be due. The undersigned can be reached at (408)777-8873 if there is any question.

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to " Mail Stop: Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450", on **April 23, 2004**.

Name: Joe Zheng

Signature: 

Respectfully submitted;


Joe Zheng
Reg.: No. 39,450